

Requested Patent: JP2000293438A

Title: METHOD FOR PROTECTING DATA OF HARD DISK DRIVE ;

Abstracted Patent: JP2000293438 ;

Publication Date: 2000-10-20 ;

Inventor(s): KAKU YOEI ;

Applicant(s): KAKU YOEI ;

Application Number: JP19990154011 19990601 ;

Priority Number(s): ;

IPC Classification: G06F12/14 ;

Equivalents: ;

ABSTRACT:

PROBLEM TO BE SOLVED: To protect the hard disk drive against breakage and theft by disabling a protection area to be written when the protection area is a read-only state or to be read when in a write-only state. **SOLUTION:** When a FORMAT command is not received, it is judged whether or not a microcontroller receives a WRITE command (step 350). When the microcontroller receives a WRITE command, it is checked whether or not an area requested to be written is a read-only protection area (step 355). If so, an alarm is given and then the WRITE command is disabled (step 345). When data requested to be written is detected, it is checked whether or not the area requested to be written is a read-only protection area (step 355); if so, an alarm is given and the data requested to be written is disabled (step 345).

【特許請求の範囲】

【請求項1】 ハードディスクドライブ中のデータを保護する方法であって、

前記ハードディスクドライブをHDDロックを介してコンピュータに接続するステップと、

前記HDDロックへ制御信号を送るステップであって、前記制御信号は、FORMATコマンド、WRITEコマンドまたはREADコマンドを含んでおり、前記制御信号は、前記FORMATコマンドによってフォーマットされる領域のアドレス、前記WRITEコマンドによって書き込みが行われる領域のアドレスまたは前記READコマンドによって読取りが行われる領域のアドレスを表す第1のパラメータを含んでいるステップと、

前記ハードディスクドライブ中に少なくとも一つの保護領域を形成するステップと、

前記保護領域のアドレスを表す第2のパラメータを記録するステップと、

前記第1パラメータを記録するステップと、

前記FORMATコマンドが受信されているときに前記第1パラメータと前記第2パラメータを比較し、前記第1パラメータが前記第2パラメータと同じ場合、そのFORMATコマンドをディセーブルにするとともに警告を与えるステップと、

前記WRITEコマンドが受信されているときに前記第1パラメータと前記第2パラメータを比較し、前記第1パラメータが前記第2パラメータと同じ場合、そのWRITEコマンドをディセーブルにするとともに警告を与えるステップと、

書き込みを要求されるデータが検出されているときに前記第1パラメータと前記第2パラメータを比較し、前記第1パラメータが前記第2パラメータと同じ場合、前記書き込みを要求されるデータをディセーブルにするステップと、

前記READコマンドが受信されているときに前記第1パラメータと前記第2パラメータを比較し、前記第1パラメータが前記第2パラメータと同じ場合、そのREADコマンドをディセーブルにするとともに警告を与えるステップと、

読取りを要求されるデータが検出されているときに前記第1パラメータと前記第2パラメータを比較し、前記第1パラメータが前記第2パラメータと同じ場合、前記読取りを要求されるデータをディセーブルにするステップと、を備える方法。

【請求項2】 前記第1パラメータは、第1のシリンダパラメータ、第1のヘッドパラメータおよび第1のセクタパラメータを含んでいる請求項1記載の方法。

【請求項3】 前記第2パラメータは、第2のシリンダパラメータ、第2のヘッドパラメータおよび第2のセクタパラメータを含んでいる請求項1記載の方法。

【請求項4】 前記第1パラメータおよび前記第2パラ

メータがメモリに記録される請求項1記載の方法。

【請求項5】 前記メモリの拡張が許されている請求項4記載の方法。

【請求項6】 前記HDDロックは、前記保護領域を書込み専用状態または読取り専用状態にするために使用されるスイッチを備えている請求項1記載の方法。

【請求項7】 前記保護領域が前記書き込み専用状態にある間、前記保護領域の読取りが禁止される請求項6記載の方法。

【請求項8】 前記保護領域が前記読取り専用状態にある間、前記保護領域の書き込みが禁止される請求項6記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ハードディスクドライブ(HDD)中のデータを保護する方法に関し、特に、保護領域を用いてデータの破壊や盗難を防ぐ方法に関する。

【0002】

【従来の技術】情報の必要性和技術の発達に伴い、コンピュータは日常生活のための重要な道具になった。ワールド・ワイド・ウェブ(WWW)の進歩と発展は、情報伝達の効率を高めている。しかしながら、コンピュータが侵入され、ウイルスによって破壊される可能性も同時に増加している。コンピュータがウイルスによって侵入されると、ハードディスクドライブ(HDD)に記録されたデータ(オペレーションシステムやファイルなど)が破壊されてしまう。さらに、ハックによってデータが破壊されたり盗まれたという問題がしばしば聞かれるようになった。したがって、ハードディスクドライブを破壊や盗難から保護することは重要である。

【0003】

【発明が解決しようとする課題】現在のところ、ハードディスクドライブの保護は、ソフトウェアプログラムのコーディング/デコーディングを通じて達成される。しかし、ソフトウェアプログラムを用いてデータを保護する上記の方法の欠点の一つは、メインメモリがプログラムを記録しなければならないということである。このため、メインメモリの多くの容量がプログラムで占められてしまう。さらに、ソフトウェアプログラムを使ってデータを保護する方法は、ウイルスの侵入を完全に避けることはできない。

【0004】ハードディスクドライブ中のデータを破壊や盗難から防ぐための積極的な態度はハックやウイルスの侵入を避けることであり、消極的な態度はデータをバックアップすることである。バックアップする方法は、一般的なディスクや高い容量を持つ別の記憶手段(MO、CD-ROM、CD-RW、リライタブルDVDなど)を使用する範囲を越えてはいない。しかし、一般的なディスクの容量は1.44メガバイトしかなく、

高い容量を有する別の記憶手段の価格は高すぎて受け入れられない。

【0005】

【課題を解決するための手段】上述の目的のために、本発明は、ハードディスクドライブ中のデータを保護する方法を本明細書のなかで開示する。データを保護する意味は、データの破壊や盗難を避けることである。ここで開示されるデータ保護方法は、ハードディスクドライブ中に少なくとも一つの特定領域を形成する。この特定領域を保護領域と名づけ、残りの領域を一般領域と名づけることにする。さらに本発明は、読取り専用状態および書き込み専用状態を含む保護領域の二種類の状態を提供する。保護領域のこれらの状態は、スイッチによって制御される。保護領域が読取り専用状態にある間、保護領域は書き込みを行うことができないので、データの破壊が回避される。保護領域が書き込み専用状態にある間、保護領域は読取りを行うことができないので、データの盗難が回避される。

【0006】上記の点や本発明に伴う利点の多くは、以下の詳細な説明を添付の図面とともに参照することによって、より容易に把握され、より良く理解される。

【0007】

【発明の実施の形態】本発明では、ハードディスクドライブ(HDD)を読取り専用(read-only)状態または書き込み専用(write-only)状態に設定することができる。本発明は、保護領域として機能する少なくとも一つの特定領域をHDD中に定義する。HDD中の残りのスペースは、一般領域と呼ぶことにする。より詳細に説明すると、読取り専用状態では、HDDへのデータ伝送が妨げられる。また、書き込み専用状態では、保護領域中のデータ記憶を読み取ることができない。

【0008】本発明のブロック図を表す図1について説明すると、本発明は、上記の目的を達成するためにHDDロック10を使用する。このHDDロック10は、コンピュータ3およびHDD5にそれぞれ接続されている。HDDロック10は、スイッチ11、マイクロコントローラ13およびメモリ15を含んでいる。スイッチ11は、HDD5の状態を切り換えるため使用され、この状態には読取り専用状態および書き込み専用状態が含まれる。より詳細に説明すると、読取り専用状態では、HDD5中のデータは読取り専用であり、保護領域は書き込みを行うことができない。このようにして、HDD中のデータの破壊を防ぐという目的が達成される。さらに、書き込み専用状態では、保護領域中のデータを読み取ることができない。このようにして、HDD中のデータ記憶の盗難を防ぐという目的が達成される。好適な態様では、スイッチ11は手動スイッチである。

【0009】さらに図1には、マイクロコントローラ13が示されている。マイクロコントローラ13は、第1のターミナル13a、第2のターミナル13b、第3の

ターミナル13cおよび第4のターミナル13dを含む四つのターミナルを有している。第1ターミナル13aは、スイッチ11に接続されている。第2ターミナル13bは、コンピュータ3に接続されている。第3ターミナル13cは、HDD5に接続され、第4ターミナル13dは、メモリ15に接続されている。図1に示されるメモリ15は、保護領域のアドレスを記憶するために使われる。このアドレスには、先頭アドレスや最終アドレスが含まれる。本発明では、IDEインタフェースHDDが好適な態様として例示される。IDEインタフェースのアドレス指定方法はCHS(シリンダ(cylinder)、ヘッド(head)およびセクタ(sector))であるから、制御信号(FORMATコマンドやWRITEコマンドやREADコマンドを含む)は、シリンダパラメータ、ヘッドパラメータおよびセクタパラメータを含んでいる。FORMATコマンド、WRITEコマンド、またはREADコマンドは、シリンダパラメータ、ヘッドパラメータおよびセクタパラメータを介して、HDD中のデータをそれぞれフォーマットし、書き込み、または読み取ることができる。本発明では、制御信号によってフォーマットされ、書き込まれ、または読み取られる領域のアドレスを第1パラメータと名づける。保護領域のアドレスも同様に、メモリ15に記録されなければならない。第1パラメータとの混同を避けるため、保護領域のアドレスを第2パラメータと名づける。この第2パラメータも、第2のシリンダパラメータ、第2のヘッドパラメータおよび第2のセクタパラメータを含んでいる。第1パラメータと第2パラメータとの比較により、フォーマットされ、書き込まれ、または読み取られる領域が保護領域であるか否かが分かる。さらに、メモリ15の容量は制限を受けない。すなわち、メモリ15の拡張が許されている。

【0010】保護領域設定ステップ200を表す図2を参照すると、保護領域はHDD中の一般領域から分離されている。ステップ200は、次のような複数のステップを含んでいる。ステップ210aでは、コンピュータが保護領域のアドレスをマイクロコントローラに送る。ステップ210bでは、マイクロコントローラが記録のために保護領域のアドレスをメモリに送る。ステップ210cでは、記録が完了したかどうか判断される。ステップ210bが完了していないときは、記録が繰り返される。ステップ210bが終了すると、ステップ210dが実行され、記録が完了したことをマイクロコントローラがコンピュータに通知する。

【0011】図3について説明する。この図は、HDD中のデータを保護する方法を示している。この方法は、次のような複数のステップを備えている。最初に、ステップ100が開始し、コンピュータが制御信号をマイクロコントローラへ送る。この制御信号は、第1シリンダパラメータ、第1ヘッドパラメータおよび第1セクタパ

ラメータからなる第1パラメータを含む可能性がある。さらに、制御信号はFORMATコマンド、WRITEコマンドおよびREADコマンドを含む可能性がある。ステップ200では、保護領域を設定するかどうかを判断される。保護領域を設定することが必要とされる場合、上述したステップ210が実行されることになる。ステップ210が終了すると、次の制御信号を受信するためにステップAが実行される。

【0012】図3をさらに参照すると、ステップ310とその次のステップが示されている。ステップ310は、マイクロコントローラが第1シリンダパラメータを受信するかどうかを判断する。第1シリンダパラメータが受信される場合、メモリが第1シリンダパラメータを記録するステップ315が実行される。第1シリンダパラメータが受信されない場合は、マイクロコントローラが第1ヘッドパラメータを受信するかどうかを判断するステップ320が実行される。第1ヘッドパラメータが受信される場合、第1ヘッドパラメータをメモリに記録するステップ325が実行される。第1ヘッドパラメータが受信されない場合は、マイクロコントローラが第1セクタパラメータを受信するかどうかを判断するステップ330が実行される。第1ヘッドパラメータが受信される場合、メモリが第1ヘッドパラメータを記録するステップ335が実行される。

【0013】図3をさらに参照すると、第1ヘッドパラメータが受信されない場合は、マイクロコントローラがFORMATコマンドを受信するかどうかを判断するステップ340が実行される。マイクロコントローラがFORMATコマンドを受信する場合は、ステップ345が実行される。ステップ345は、警告を与えてからFORMATコマンドをディセーブルにする。

【0014】図3をさらに参照すると、FORMATコマンドが受信されない場合、マイクロコントローラがWRITEコマンドを受信するかどうかを判断するステップ350が実行される。マイクロコントローラがWRITEコマンドを受信する場合は、書き込みを要求される領域が読取り専用保護領域であるか否かをチェックするステップ355が実行される。書き込みを要求される領域が読取り専用保護領域である場合、警告を与えてからWRITEコマンドをディセーブルにするステップ345が実行される。このようにして、データを破壊から保護する目的が達成される。これに対して、書き込みを要求される領域が読取り専用保護領域でない場合は、WRITEコマンドをHDDに送ってHDDを起動するステップ390が実行される。書き込みを要求される領域が読取り専用保護領域であるか否かを判断する方法は、メモリに記録された第1パラメータと第2パラメータとの比較を行うことによって達成される。

【0015】図3をさらに参照すると、WRITEコマンドが受信されない場合、書き込みを要求されるデータが

受信されるかどうかを判断するステップ360が実行される。このステップ360は、HDD中のデータの破壊を防ぐための二重チェックとして働く。書き込みを要求されるデータが検出されると、書き込みを要求される領域が読取り専用保護領域かどうかをチェックするステップ355が実行される。書き込みを要求される領域がちょうど読取り専用保護領域である場合、警告を与えてから書き込みが要求されるデータをディセーブルにするステップ345が実行される。このようにして、データを破壊から保護する目的が達成される。これに対して、書き込みを要求される領域が読取り専用領域でない場合は、WRITEコマンドにHDDを送ってHDDを起動するステップ390が実行される。書き込みを要求される領域が読取り専用保護領域であるかどうかを判断する方法は、メモリに記録された第1パラメータと第2パラメータとの比較を行うことによって達成される。

【0016】図3をさらに参照すると、書き込みを要求されるデータが受信されないとステップ360が判断した場合、マイクロコントローラがREADコマンドを受信するかどうかを判断するステップ370が実行される。マイクロコントローラがREADコマンドを受信する場合、読取りを要求される領域が書き込み専用保護領域であるかどうかをチェックするステップ375が実行される。読取りを要求される領域がちょうど書き込み専用保護領域である場合、警告を与えてからREADコマンドをディセーブルにするステップ345が実行される。このようにして、データを盗難から保護する目的が達成される。これに対して、読取りを要求される領域が書き込み専用保護領域でない場合は、READコマンドがHDDへ送られ、HDDが起動される。読取りを要求される領域が書き込み専用保護領域であるか否かを判断する方法は、メモリに記録された第1パラメータと第2パラメータとの比較を行うことによって達成される。

【0017】図3をさらに参照すると、READコマンドが受信されない場合、読取りを要求されるデータが受信されるかどうかを判断するステップ380が実行される。読取りを要求されるデータがマイクロコントローラによって検出されると、読取りを要求されるデータが取り出される領域が読取り保護領域であるかどうかをチェックするステップ375が実行される。読取りを要求されるデータが取り出される領域がちょうど書き込み専用保護領域である場合、警告を与えてからREADコマンドをディセーブルにするステップ345が実行される。このようにして、データを盗難から保護する目的が達成される。これに対して、読取りを要求されるデータが取り出される領域が書き込み専用保護領域でない場合は、読取りを要求されるデータがコンピュータへ送られる。読取りを要求される領域が書き込み専用保護領域であるか否かを判断する方法は、メモリに記録された第1パラメータと第2パラメータとの比較を行うことにより達成される。

る。読取りを要求されるデータがマイクロコントローラによって受信されない場合は、制御信号をHDDへ送るステップ390が実行される。

【0018】ここで開示した方法はSCSIインタフェースにも適していることが注目される。ここで、SCSIインタフェースのコマンドシーケンスを表す図4を参照する。制御信号がFORMATコマンド、WRITEコマンド、READコマンドのいずれを表しているかは、C/D、SEL、I/O、MSGなどのSCSI制御信号によって決まる。シリンダパラメータ、ヘッドパラメータまたはセクタパラメータは、論理ブロック (Logical block) のデコーディングを通じて決定される。第1パラメータと第2パラメータとを比較した後、フォーマット、書き込みまたは読取りを要求される領域が保護領域であるか否かが判断される。フォーマット、書き込みまたは読取りを要求される領域が保護領域である場合、データを保護するために制御信号がディセーブルにされる。

【0019】当業者であれば理解できるように、上述した本発明の好適な実施形態は本発明の例示であり、本発明を限定するものではない。請求項の趣旨と範囲に含まれる種々の変形例や類似の構成を包含することが意図されており、ここで請求項の範囲は、このような変形例や類似構造のすべてを包含するように最も広い解釈に一致させるべきである。

【図面の簡単な説明】

【図1】本発明に係るブロック図である。

【図2】保護領域を設定するためのステップを表す図である。

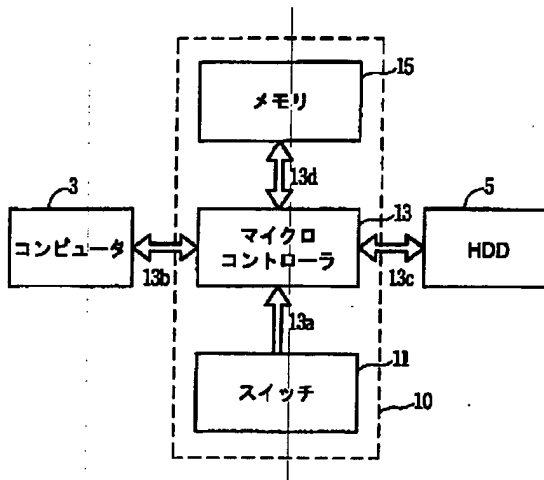
【図3】本発明に係るフローチャートである。

【図4】SCSIインタフェースのコマンドシーケンスを列挙する図である。

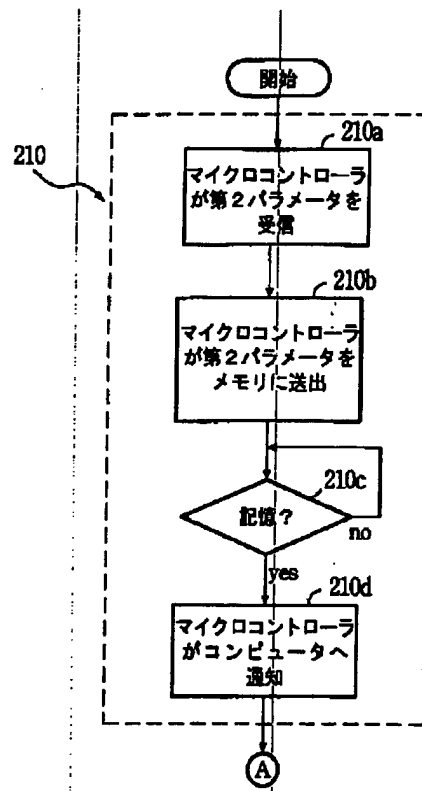
【符号の説明】

3…コンピュータ、10…ロック、11…スイッチ、13…マイクロコントローラ、13a～13d…ターミナル、15…メモリ。

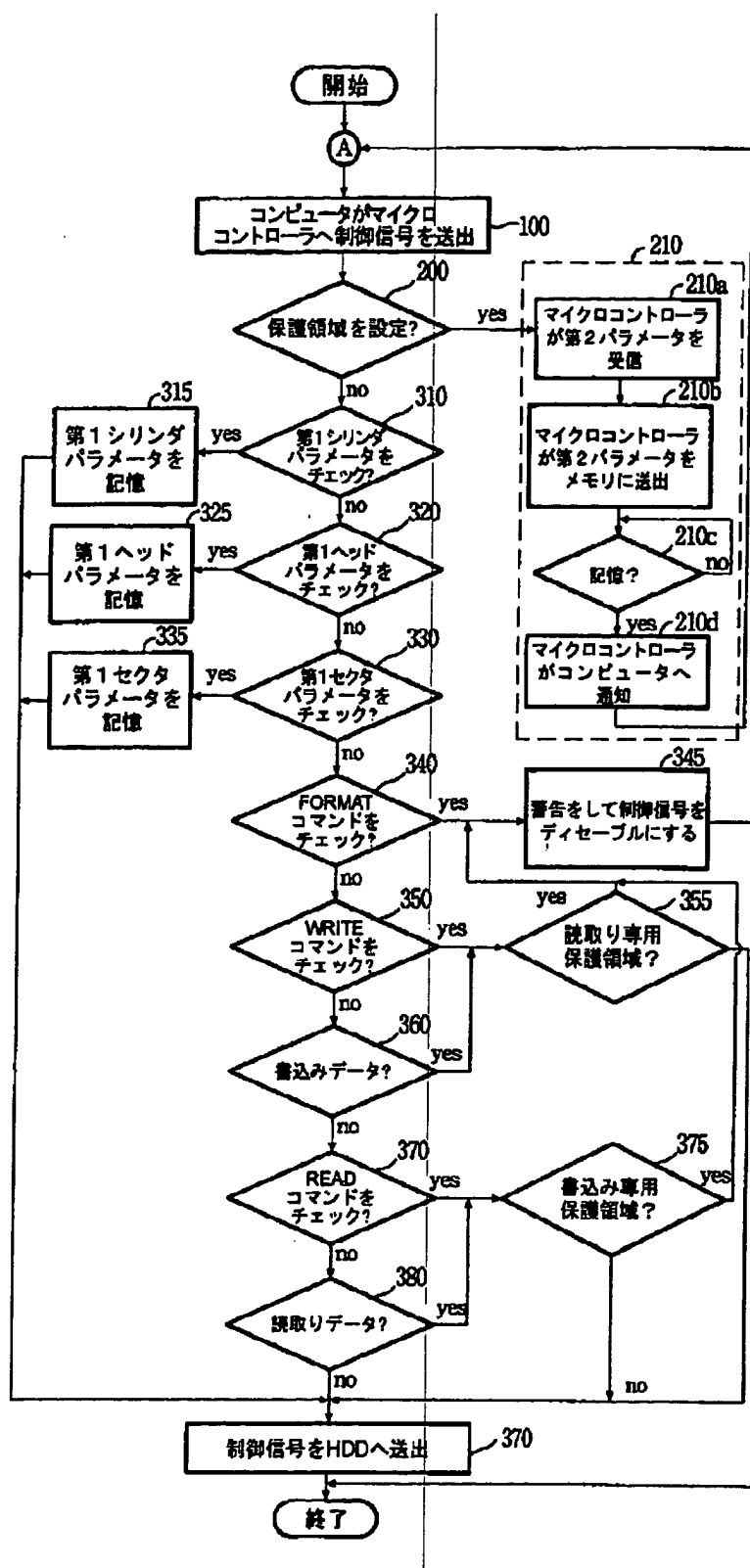
【図1】



【図2】



【図3】



【図4】

	7	6	5	4	3	2	1	0
0	Read or Write							
1	(LUN)		DPO	FUA	Res.		Rel	
2	Logical block							
3								
4								
5								
6	Reversed							
7	Data length							
8								
9	Control byte							